

REMARKS/ARGUMENTS

Claims 1-3, 6, 7, 9, 11, 13, 20-22, 25 and 26 are being resubmitted. Claims 1, 9 and 20 are currently amended. Claims 8 and 27 have been canceled. No new claims are being added.

Claims 1-3, 6-9, 11, 13, 20-22, 25 - 27 were rejected under 35 U.S.C 103(a) as being unpatentable over U.S. Patent Application Publication No. 2002/0073047 A1 to Morrison (Morrison), in view of U.S. Patent Application Publication No. 2003/0204515 A1 to Shadmon et al. (Shadmon) and further in view of U.S. Patent No. 7,095,850 B1 to McGrew (McGrew).

Amendments to the Claims

Claim 1 has been amended to recite:

“digitizing and organizing lectures in an e-learning system to produce the digital assets”, the amendment being supported, for example, in paragraph [0023];

“wherein a text string identifying a node in the tree structure is generated by appending text to a text string identifying the node’s parent node”, the amendment being supported, for example, at paragraphs [0023] and [0026] and Figure 1;

“wherein the one way function is responsive to the text string identifying a node”, the amendment being supported, for example, at paragraphs [0026] and [0031];

“providing the one way function at the digital asset client either by communicating from the digital asset server to the digital asset client or by embedding the one way function at the digital asset client”; the amendment being supported, for example, at paragraph [0030];

“generating, at the digital asset client, keys for descendent nodes of a group node, responsive to the group node’s key and the one way function”; the amendment being supported, for example, at paragraph [0025];

Claim 9 has been amended to recite:

“digitized lectures in an e-learning system”, the amendment being supported, for example, at paragraph [0006], Figure 1 and Figure 2

“(e) an input interface unit for accepting instructions from an administrator; the instructions comprising: modifying the tree structure, changing content of the asset, regenerating a root key and computing a cipher key at a node;” the amendment being supported, for example, at paragraph [0055];

“wherein said root node represents a main course and said leaf nodes represent lectures in various courses;” the amendment being supported, for example, at paragraph [0023];

“wherein the decrypting unit generates keys for descendent nodes of a group node using the group node’s key and the predetermined one-way function”; the amendment being supported, for example, at paragraph [0025];

Claim 20 has been amended to recite:

“creating the digital assets by digitizing lectures”, the amendment being supported at paragraph [0006];

“responsive to a text string identifying the root node”, the amendment being supported at paragraph [0031]

“providing a one-way function from the digital asset server to the digital asset client;” the amendment being supported, for example, at paragraph [0030];

“checking by an authentication process if a digital asset client requesting an asset is a legal user of the asset;” the amendment being supported, for example, at paragraph [0054];

“accepting instructions from an administrator through an input interface; the instructions comprising one or more of: modifying the tree structure; adding, amending, or deleting asset contents; regenerating a root key; computing keys of various nodes at various levels; and encrypting modified asset content;” the amendment being supported, for example, at paragraph [0055].

Morrison in view of Shadmon further in view of McGrew

Claims 1-3, 6-9, 11, 13, 20-22, 25 - 27 were rejected under 35 U.S.C 103(a) as being unpatentable over U.S. Patent Application Publication No. 2002/0073047 A1 to Morrison (Morrison),), in view of U.S. Patent Application Publication No. 2003/0204515 A1 to Shadmon et al. (Shadmon) and further in view of U.S. Patent No. 7,095,850 B1 to McGrew (McGrew).

Morrison discloses a method for “conducting a transaction over a network” (abstract). In particular, the claimed method is useful because “Rather than requiring a client to pay for the downloadable file first and then transferring the file, the present invention allows a client to pay for a decryption key after an encrypted file has been downloaded.” Morrison does not fairly teach suggest or motivate organization of downloadable files as a tree structure using the naming scheme of the present invention, wherein every node of the tree structure at a lower level is identified by appending to the text string identifying its parent node. Morrison also does not fairly teach, suggest or motivate use of his invention to e-learning system offering downloadable digitized lectures.

Even if Morrison is combined with Shadmon in the sense of “organizing data in a tree structure, wherein the root node of the tree represents all assets” (Office Action, page 4, item 12), the combined references still do not fairly teach, suggest or motivate application to the e-learning field, because Shadmon is merely concerned with “[a] method for encoding hierarchical data stored in an index, partitioned into blocks, over keys representing the data” (abstract) and “indexing and accessing semistructured data and hierarchical data” (Field of Invention). Moreover, Shadmon does not teach how to index nodes by assigning textual labels to the nodes as disclosed in the present invention.

Even if Morrison and Shadmon are combined with McGrew in the sense of “randomly generating a key for root node” (Office Action, page 4, item 14) or “computing different keys for two nodes having the same father node” (Office Action, page 5, item 16), McGrew is concerned with “forward secrecy by updating a key by using a one-way function after each encryption” (abstract). Regarding selection of the function at a node, McGrew states “In one embodiment, the number m of bits of state per node, and the key size, are specified by parameter values. The parameterizable width enables reduced size versions of the cipher to be studied, enabling numerical experiments on the cipher to be more meaningful. The parameterizable key size is useful to adapt the cipher to different security policies, and to protect against typical plaintext attacks by enabling keys to be increased in size to compensate for the possibility of cryptographic attacks that use precomputation” (column 9, lines 22-27) or “in one embodiment, m [bits of state per node] is restricted to being a multiple of twelve” (column 9, lines 35-36). Thus, McGrew does not fairly teach, suggest or motivate the text labeling scheme of the present invention. Neither does McGrew provide any comments or suggestions regarding suitability of their invention to e-learning use of the present invention.

Therefore, the combined teachings of Morrison, Shadmon and McGrew do not render obvious a method of generating hierarchical keys for digital assets comprising:

“digitizing and organizing lectures in an e-learning system to produce the digital assets”,

“wherein a text string identifying a node in the tree structure is generated by appending text to a text string identifying the node’s parent node”,

“wherein the one way function is responsive to the text string identifying a node”,

“providing the one way function at the digital asset client either by communicating from the digital asset server to the digital asset client or by embedding the one way function at the digital asset client”

“generating, at the digital asset client, keys for descendent nodes of a group node, responsive to the group node’s key and the one way function”

as claimed by the amended Claim 1; or

“digitized lectures in an e-learning system”;

“(e) an input interface unit for accepting instructions from an administrator; the instructions comprising: modifying the tree structure, changing content of the asset, regenerating a root key and computing a cipher key at a node;”

“wherein said root node represents a main course and said leaf nodes represent lectures in various courses;”

“wherein the decrypting unit generates keys for descendent nodes of a group node using the group node’s key and the predetermined one-way function”

as claimed by the amended Claim 9; or

“creating the digital assets by digitizing lectures”,
“responsive to a text string identifying the root node”,
“providing a one-way function from the digital asset server to the digital asset client;”

“checking by an authentication process if a digital asset client requesting an asset is a legal user of the asset;”

“accepting instructions from an administrator through an input interface; the instructions comprising one or more of: modifying the tree structure; adding, amending, or deleting asset contents; regenerating a root key; computing keys of various nodes at various levels; and encrypting modified asset content;”

as claimed by the amended Claim 20.

Thus, Applicant respectfully submits that Morrison in view of Shadmon further in view of McGrew does not make obvious the present invention and the section 103 rejection should be withdrawn.

CONCLUSION

Reconsideration and withdrawal of the Office Action with respect to Claims 1-3, 6, 7, 9, 11, 13, 20-22, 25 and 26 is requested. Applicants submit that the claims are now in condition for allowance or at least in better form for appeal. Applicants respectfully request that a timely Notice of Allowance be issued in this case.

In the event the examiner wishes to discuss any aspect of this response, please contact the attorney at the telephone number identified below.

Appl. No. 10/825,913
Amdt. dated Dec 31, 2007
Reply to Office action of Nov. 14, 2007

☒ The Commissioner is hereby authorized to charge payment of the following fees with this communication or credit any overpayment to Deposit Account No. 09-0441:

☒ Any filing fees under 37 CFR 1.16 for the presentation of extra claims.

Respectfully submitted,

By: /Vinay Sathe /
Vinay Sathe
Agent Registration No. 55,595
Michael A. Shimokaji
Attorney Registration No. 32, 303

SHIMOKAJI & ASSOCIATES, P.C.
8911 Research Drive
Irvine, CA 92618
(949) 788-9961